**5-2 Coding Assignment: Certificate Generation**

Winnie Kwong

Southern New Hampshire University

CS-305 Software Security

Professor Foultz

September 30th, 2023

**Certificate Authorities**

**Roles & Values**

Certificate Authority (CA) helps to prove which organization or person can be trusted when providing personal or payment information. When acquiring a CA, a browser must create a Certificate Signing Request with their key pair. Once an entrusted partner signs the request with a private key, anyone with access to the public key can verify the CA was signed. (Kubucation, 2019, 11:01). A CA's Key roles are to issue digital certificates and maintain a list of untrustworthy ones. Having a digital certificate means one's contact information is validated and can provide users with confidence of integrity. A certificate revocation list (CRL) helps to maintain which sites are untrustworthy because it helps to determine if the sites have expired dates or if their private keys have been compromised.

**Security Purposes**

While CA verifies how authentic or trustworthy a website or person can be, it also has many security purposes. Website owners are responsible for securing their sites from being stolen, read, or modified by attackers. According to Pagano, the value of CA is equivalent to an “exclusive club,” because it requires a lot of work to maintain a forever trust with software vendor standards. (Pagano, 2019, Para 5). When enforcing industry standards, internet security is strengthened and prevents end users from malicious attacks. A lock icon under the search engine indicates if a website has a secure network connection with CA. If the lock is unlocked, the communication network is unsafe and can be tampered with or eavesdropped on by third parties. When browsing a website, public keys are distributed for anyone to read. However, with CA, the public key creates an encrypted private key to protect the communication channel between both machines. Only users with the private key can decrypt the message to access the communication channel.

**Advantages**

There are a number of benefits when it comes to CA such as validation and relief. CA can provide validation assurance when using the website. Using CA can establish more information about the owner, such as their location or domain ownership just by performing extensive checks. (Coclin, 2021, para 4). Knowing a person’s or organization’s identity is important because it provides a sense of reliability when knowing if the end user’s data could be threatened by bugs or other malware attacks. CA provides relief to businesses because partners would handle the burden of maintaining a private CA. Websites would need to focus on compliances or other security issues, but partners would have tools to simplify the process. Using certificates such as SSL helps to keep encryption stable for data security for all business components.

**Completed Form**

A screenshot of a computer screen

Description automatically generated

**Certificate**

A computer screen with white text

Description automatically generated

References

Coclin, D. (2021, June 26). *What Is a Certificate Authority? | CA’s Explained | DigiCert*. Www.digicert.com. <https://www.digicert.com/blog/what-is-a-certificate-authority>

Kubucation (2018, April 1). *How does HTTPS work? What's a CA? What's a self-signed Certificate?* YouTube. Retrieved September 28, 2023 from <https://www.youtube.com/watch?v=T4Df5_cojAs>

Pagano, E. (2019, December 23). *What is the Value of Certificate Authorities?* www.SSL.com. Retrieved September 27, 2023, from <https://www.ssl.com/article/value-of-certificate-authorities/#:~:text=On%20a%20fundamental%20level%2C%20CA>

‌

‌